

REMARKS

At page 2 of the Office Action, the Examiner rejected claims 13, 41 and 56 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In particular, the Examiner stated that the term “some intended overlap” is a relative term. Accordingly, the Applicant has amended claims 13, 41 and 56 to replace “some intended overlap” with “an overlap of at least a portion of information that is common to two or more of the plurality of sub-puzzles”. This amendment is supported in the specification, for example at page 31.

At page 3 of the Office Action, the Examiner rejected claims 1-10, 14-22, 24-38, 42-53 and 57-59 under 35 U.S.C. 103(a) as being unpatentable over Liao et al. in view of R.C. Merkle and in further view of Benson. The Applicant respectfully disagrees, for at least the following reasons.

At ¶2, the Examiner states that Liao teaches step (b) of claim 1, “imposing on said client a computational task and a time limit for correct completion of said computational task” at col. 7, lines 5-25 and col. 10, lines 22-37. Col. 7, lines 5-25 of Liao describes a mutual authentication transaction between a server and a client. This text does not teach or suggest a computational task imposed on the client as part of the mutual authentication process, nor does it teach or suggest any time limit for completion of a task. Col. 10, lines 22-37 describes an action a client performs to complete a session creation process, in particular sending a “session complete” (SC) message. However, this action is not imposed upon the client, but rather is part of a transaction between the client and the server. Further, this text does not teach or suggest a time limit for the action the client performs.

Step (b) of claim 1 is recited in addition to and in association with step (a), which calls for “receiving a resource allocation request from the client. The Examiner states that Liao teaches step (a) at col. 12, lines 46-63. This text describes a client initiating a service transaction by sending a service request (SR) to a server, but does not teach or suggest any request from the client for allocation of any resources. Initiating a service transaction cannot be construed as a request for resource allocation, since such a transaction as described by Liao does not encompass any resources of which the client could request allocation.

The Examiner also states that Liao teaches step (d) of claim 1, “allocating said resource for said client if the verification is received” at col. 12, lines 19-25 and lines 63-66. The “verification” in this claim is defined in step (c) of claim 1 as the verification that the client has correctly performed the computational task within the time limit. The text in Liao at col. 12, lines 19-25 and lines 63-66 describes completion of an authentication transaction, but does not teach or suggest verification any activity within a time limit, and so does not teach or suggest verification that the client performed a computational task within a time limit. In fact, the Examiner states at page 4 that Liao does not explicitly disclose that the client has correctly performed a computational task within a time limit.

The Examiner further states that Merkle combined with Liao teaches at least some of the claim 1 limitations not taught by Liao alone, in particular “receiving verification that the client has correctly performed the computational task within a time limit.” Merkle teaches using a set of puzzles to allow two parties to agree on a key with which to encrypt further communications, while making it difficult for a third party to determine the key. Merkle does not teach or suggest any sort of time limit for solving the puzzle, nor does it teach or suggest the successful solution of the puzzle for allocation of anything to a client. The puzzle described in Merkle is merely a way to prevent an unwanted third party from acquiring a key, and is not used as a task imposed on a client that the client must successfully perform to be allocated resources. Thus Merkle does not teach or suggest receiving verification that a client has correctly performed the computational task within a time limit as claim 1 requires. The Examiner states that Merkle discloses “a method creating a puzzle of varying complexity during challenge response communication (page 296 co. 1, 2nd paragraph to end of col. 2) in order to thwart a denial-of-service attack.” (emphasis added). However, Merkle is not directed to denial-of-service attacks, and there is nothing in Liao or Merkle to motivate one to combine these references. Since no motivation exists for combining these references, the Examiner improperly combines Liao with Merkle for this rejection.

The Examiner further states that Benson combined with Liao and Merkle teaches the time limit for correct completion of the computational task recited in steps (b) and (c) of claim 1. Benson teaches a way to use asymmetric cryptography (public key/private key) to provide an electronic copy protection mechanism. The Examiner states that Benson at col. 11, lines 19-30

discloses that an executable response is time bound requiring the client to execute the response within a predetermined amount of time. In this text, however, Benson describes a way to ensure “freshness” of a copy protection protocol that uses a challenge/response exchange, so that an attacker cannot thwart the copy protection protocol by replaying old messages. In Benson, the “challenge mechanism validates both freshness of the timestamp and correctness of the signature” (col. 11, lines 26-28, emphasis added). The challenge mechanism is part of the copy-protected software, and is therefore located with the customer (*i.e.*, the client), so in Benson it is the client that is validating the timestamp (see, for example, col. 4, lines 16-29; col. 5, lines 11-17). This is significantly different from what is described in the specification and claimed in claim 1, where a computational task is imposed on the client, and a server validates whether the client performed the task within a time limit. Therefore neither Liao, nor Merkle, nor Benson teaches or suggests a time limit for correct completion of a computational task as recited in steps (b) and (c) of claim 1.

For at least these reasons, the Examiner’s rejection of claim1 under 35 U.S.C. 103(a) as being unpatentable over Liao et al. in view of R.C. Merkle and in further view of Benson is improper and should be withdrawn. Similarly, the rejection of independent claims 18, 27 and 47 are improper and should be withdrawn, since these claims all include the elements of the claim limitations described above.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: November 17, 2005

Respectfully submitted,

By 

Ronald R. Demsher

Registration No.: 42,478

WILMER CUTLER PICKERING HALE AND
DORR LLP

60 State Street

Boston, Massachusetts 02109

(617) 526-6000

Attorney for Applicant